REMARKS/ARGUMENTS

Please reconsider the application in view of the above amendments and the following remarks. Applicants thank the Examiner for carefully considering this application.

Claims 1 through 12 are in this application. Claims 1 though 10 remain from the initial filing. Applicant has new added claims 11 and 12.

Claim Rejections

Claim 1 is rejected under 35 USC 103(a) as being unpatentable over Bishop, and further in view of Abraham et al (US patent 5,539,906). Applicant respectfully traverses the Examiner's assertion.

Applicant's present invention describes a privilege transfer method between programs in a computing system. In this method the system's native privileged user may start a program (such as a security manager) on the system. Subsequently, the privilege to administer the new program is transferred from the native privileged identity to a designated user identity. Once transferred, the initial privileged identity, the system's native privileged user, losses privilege with respect to the program (security manager) and the new registered identity gains administrative control over the program (security manager). Since the new registered identity is not the native root identity.

As discussed in the specification, one need with regard to the implementation of a security manager is establishing a model in order to apply the security manager to a computing system and then prevent the normal operating system (OS) administrative user from potentially disabling or administering the external manager without the required privilege. Applicant's present invention provides this solution.

The Examiner asserts that Bishop teaches the method for transferring and monitoring privilege access to functions in a computing system. On the Unix Security Paper (Bishop), Applicant submit that there is no relationship between the materials discussed in Bishop to the present application. The paper discusses several relevant security topics in super computing, existing Unix technology, and recommended best

practices. Applicant sees two topics in the paper that perhaps might be considered to have some relevance to Applicant's present application. One is the discussion on assigning specific administrative tasks to different user accounts instead of the all powerful Unix super user account. The other is the notion that modification of a privileged program (setuid program) causes it to lose its setuid capability. However, neither of these topics is related to the key concepts of the present application, which are transfer of privilege from one program and identity to another program and identity, loss of privilege to the initiator of the privilege transfer, and inheritance of privilege to descendents of the new privileged program.

Similarly, Applicant submits that the techniques described in the Abraham patent do not describe the methods in the present privilege transfer application. Abraham does describe steps where changes to security categories on data change what groups of users can access the data. In that sense, access capabilities on the data change as the data moves through a set of processing steps (industrial process) that change the security categories on the data. This is not the nature of the techniques in the present privilege transfer application. The privilege transfer application techniques involve transfer of privilege to control an application and its related data based on the involved identities and associated programs, not any properties of the application or the data. Applicant believes these techniques are different and unique from the approaches of Abraham. They are identity based and not data based. Key methods of the invention are:

1. Initiation of privilege transfer to manage a target running application (resource manager) by a highly privileged system identity (e.g. Unix superuser). Only this highly privileged user can initiate the transfer.
2. Hand-off of privilege to another program and all its descendents along with the receiving program's established identity, which does not have any system administration privileges.

3. After the transfer (hand-off), the initiator of the transfer loses all authority to manage or interfere with the operation of the involved resource manager. Even though the initiator has all privileges to manage the system, it is cannot to subvert the operation of the involved resource manager or alter characteristics for any resources it controls.

4. After the transfer of privilege, the receiver of the privilege retains the privilege until it chooses to release the privilege by terminating all its uses of the privilege. This happens when the program that received the transfer of privilege and all the program's descendent programs terminate.

Applicant submits that none of the above 4 key aspects of the present invention are present in the references cited by the examiner. Applicant submits that the material in cited references, independently or in combination, does not produce an obvious path the techniques of the Applicant's present privilege transfer application.

The Donovan reference, it seems to be centered on caching and re-use of a successful authentication from a terminal for a limited number times if terminal properties match the cached state. Applicant submits that one can assume the count aspect from this patent is similar to the maintained count described in the present invention. However the two described counting mechanisms are different. In Donovan the count is used as a limit on the number of times the cached state is used before the cache is considered invalid and access to the central authentication authority is required. In Applicant', the count tracks the number of outstanding uses of the privileged identity after the transfer. When the use count drops to zero the privileged identity goes out of effect and privilege returns to the system administrative super user. So the count concepts have entirely different purposes

The Examiner asserts that the concept of initializing a program having a system privilege and transferring that privilege from the native OS to a designated user and then disabling that OS from disabling that privilege is not a claimed invention. Although the

claim is not worded as such, the second step of claim 1 states the transferring the privilege away from the system program that had the privilege during the initialization of the resource manager. This step is described in paragraphs [0024] and [0025] of this published application (2002/0078378). As stated [0025], the intent is to start the security manager with root and then transfer the administrative privilege of the manager to an identity that was designed to administer the security manager. The root would lose this privilege after the transfer. If the Root were able to control the security manager, this control by Root could compromise the security that the manager provides. Applicant has added new claims 11 and 12 to better cover this limitation.

As mentioned, the Bishop reference describes UNIX security in a Supercomputing Environment. The sections cited by the Examiner under the Access, Control, Integrity and Least Privilege section. This section discusses some alternatives to the standard UNIX security mechanism. However, the sections cited on pages 695 and 696 do not address in any way the concepts of initializing a program having a system privilege and transferring that privilege from the native OS to a designated user, and then disabling that OS from disabling that privilege. This section does discuss methods to limit the capabilities of what is described as the super user, but does not teach or suggest any of the techniques of Applicant's present invention.

Abraham (5,539,906) discusses controlling access to elements in a data processing system based on the status of a process. This system allows certain users to access predetermined elements based the step of a process that is currently active.

For there to be obviousness, there must something that teaches or suggest the combination. Bishop discusses security processes that may serve as alternatives to standard UNIX processes. There is nothing in Bishop that teach or suggest the concepts in Abraham. Applicant further submits that even if there were a combination of the teachings of Bishop and Abraham, that combination does not describe, teach or suggest the concepts and techniques of Applicant's present invention. Donovan does not mention privilege counts. Further describes techniques for validating access of hardware

(terminals). In this way, Donovan is non-analogous art with regard to both Bishop and Abraham. It does discuss access count, but that mentioning does not imply any relation to Bishop or Abraham. There is nothing in Abraham or Bishop to suggest the combining of these references. Additionally, a combination of these references does not teach or suggest Applicant's present invention.

Obviousness cannot be established by combining the teachings of cited references to produce the claimed invention, absent some teaching, suggestion or incentive supporting the combination. *In re Geiger* (Fed. Cir. 1987). In other words, elements of separate patents cannot be combined where there is no suggestion of such combination. As previously stated, there is nothing in the references separately or combined that even discuss the concept of having a privilege in one program during initialization, then transferring that to another program and away from the program that had the privilege during the initialization process. Further, there must some reasonable expectation of success.

In view of the above explanation, Applicants respectfully submit that none of the art of record (alone or in combination) teaches, discloses or even suggests the invention as recited in each of Applicant's claims. Applicant further submits that all of the pending claims are in condition for allowance. Withdrawal of the rejections and passage to issuance is respectfully requested. Applicant believes this reply to be fully responsive to all outstanding issues and place this application in condition for allowance. If this belief is incorrect, or other issues arise, do not hesitate to contact the undersigned at the below listed telephone number.

Respectfully Submitted,

Darcell Walker
Reg. No. 34,945
9301 Southwest Freeway, Suite 250
Houston, Texas 77074
713-772-1255
June 3, 2005